

Die Virtuelle Poststelle - auf der Suche nach einem Phantom?

von Martin Weinberg*

EINLEITUNG

Kaum ein anderes Thema im Umfeld von laufenden eGovernment-Projekten hat in den letzten Jahren mehr für Verwirrung und Diskussionsstoff in Deutschland gesorgt, als das der Virtuellen Poststelle, die auch unter der Abkürzung VPS, bekannt ist. Unzählige Abhandlungen, Berichte, Flyer und Fachvorträge sind veröffentlicht worden. Suchmaschinen finden über 8.000 Dokumente, die den Begriff „*Virtuelle Poststelle*“ beinhalten.

Umso erstaunlicher ist es, dass der Versuch, eine allgemeingültige Definition einer Virtuellen Poststelle zu bekommen, scheitert. Auf die Anfrage „*Define: virtuelle Poststelle*“ liefert Google keine verwertbaren Ergebnisse. Es existiert bisher keine Definition, die festlegt, was eine Virtuelle Poststelle ist.

Die ausbleibende Antwort kann als Indiz gelten für die Unklarheit, in der sich die Diskussion um und über die Virtuelle Poststelle befindet. Der Begriff wird nach Belieben interpretiert, technische, organisatorische und rechtliche Themen werden in den Mittelpunkt der Diskussion gestellt oder miteinander vermengt. So geht der ursprünglich klar umrissene Ansatz verloren. So gilt es heute mehr denn je, den roten Faden wiederzufinden, aufzunehmen und Praktikern in der Verwaltung zu helfen, sich in der verwirrenden Vielfalt im Umfeld der Anwendung VPS zurechtzufinden.

HISTORIE

Einen einfachen Zugang zu dem Thema Virtuelle Poststelle ist möglich, wenn man sich die Entwicklungsschritte ansieht, die bisher genommen wurden.

GESTERN

Entstanden ist der Begriff während des [Media@Komm-Projektes](#), das den Anspruch hatte, das „virtuelle Rathaus“ in Deutschland Realität werden zu lassen. Ein zentraler Baustein war: Sicherheit durch den Einsatz von Verschlüsselungstechnologie zu schaffen und ein Basisprotokoll zu entwickeln, auf dem Transaktionen und Programme mit höherem Sicherheitsanspruch aufsetzen konnten.

Der Begriff der Virtuellen Poststelle - kurz VPS - wurde erstmals im Jahr 2000 auf der Webseite der **bremen online-services GmbH & Co.KG (bos)** benutzt. Die erste VPS war eine in der Programmiersprache Java entwickelte Anwendung, mit der ein strukturierter Text mit Hilfe einer Smartkarte (Signaturkarte) signiert und verschlüsselt an einen Server geschickt werden konnte. Der Server wurde Intermediär genannt, Protokoll und weitere Infrastrukturkomponenten die zum Betrieb der Anwendung nötig waren, bekamen dem Namen OSCAR (**OCSI-Architektur**). Bei OSCI-Transport kommunizieren zwei Kommunikationspartner, die sogenannten OSCI-Benutzer, niemals direkt miteinander, sondern stets über die Vermittlungsstelle (Intermediär). Hauptaufgabe des Intermediär ist es, für die beiden Partner, die nicht notwendigerweise Menschen, sondern vielmehr Programme oder Softwarekomponenten sind, eine neutrale Vermittlungsinstanz zu bieten, der beide Partner vertrauen können. Technisch spricht man von einer Rolle, die der Intermediär übernimmt.

Für das weitere Verständnis ist es wichtig zu wissen, dass eine VPS - trotz des Namens - deshalb nicht im Sinne der bekannten e-mail-Kommunikation zu verstehen ist, sondern nur als Basistechnologie für rechtssicheres eGovernment. Eine VPS besteht aus aufeinander abgestimmten Komponenten. Absender (Client), Intermediär (Vermittler) und Empfänger (Backend) kommunizieren miteinander über ein gemeinsames Protokoll, das durch die Nutzung der elektronischen Signatur geschützt wird. IT-Fachleute sprechen von **Middleware**.

Übertragen in die reale Welt ist die VPS das elektronische Äquivalent zum „Nachbriefkasten“, so wie er an vielen Stellen anzutreffen ist. Dokumente können direkt, ohne über den Verteilerweg der Post zu laufen, kurzfristig übermittelt werden. Der Absender vertraut darauf, dass der Nachbriefkasten durch die

vertrauenswürdige Instanz (die Kommune) rechtzeitig geleert wird und die Schriftstücke auch bearbeitet werden. Kein Mensch würde aber die Postkarte an Tante Elfriede mit der Nachricht des bestandenen Führerscheins in den Nachtbriefkasten einer Kommune werfen, wenn er sicherstellen will, dass Tante Elfriede auch wirklich die Finanzierung des neuen Autos übernimmt.

VORBILD

Vorbild für die Architektur und den neuen Typus von Anwendungen war das *Elektronic Banking*. Der Zentrale Kreditausschuss (ZKA) hatte 1997 das Protokoll **HomeBanking Computer Interface (HBCI)** definiert. HBCI gilt als sicherer Standard sowohl für den internen Datenverkehr in der Bank-IT als auch für den Transport zum Kunden. Um Sicherheit zu gewährleisten wird der Datenverkehr dabei zwischen Kunde und Bank verschlüsselt. Der Schlüssel kann entweder auf einer Diskette oder aber auf einer Smartkarte, für die man einen Chipkartenleser benötigt, abgelegt werden. Gleichzeitig ist es möglich, neben den strukturierten, genormten Transaktionsdaten auch freie Nachrichten an das Kreditinstitut zu übertragen.

OSCAR DER ERSTE PROTOTYP

Diese erste VPS (**OSCAR**) hatte die Funktion, strukturierte Kommunikationsdaten zu signieren und diese Daten an den Intermediär zu übertragen. Nach Prüfung und temporärer Zwischenspeicherung reichte der Intermediär die Daten an den eigentlichen Empfänger weiter. Die Techniker sprachen dabei von zeitversetzter (**asynchroner**) Kommunikation mit dem Basisprotokoll, das **OSCI (Online Services Computer Interface)** genannt und als Pendant zum HBCI verstanden wurde. Durch OSCI wurden die notwendigen technischen Voraussetzungen implementiert, die für rechtssichere und verbindliche Transaktionen zwischen öffentlichen Dienstleistern und anderen Verwaltungen oder externen Anwendern notwendig sind. OSCI ist ein Transportprotokoll mit den Zielen: Integrität, Authentizität, Vertraulichkeit und Nachvollziehbarkeit bei der Übermittlung von Nachrichten zu gewährleisten.

PRINZIPIEN DES TRANSPORTPROTOKOLLS

OSCI Transport beruht - vereinfacht dargestellt - auf dem Prinzip von **doppelten Umschlägen**. Die signierte Nachricht wird zweimal verschlüsselt, einmal für den Empfänger und ein zweites Mal zum Transport. So kann der in der OSCI-Spezifikation vorgesehene zentrale Vermittler (**Intermediär**), den ersten Umschlag öffnen, entschlüsseln und prüfen. Die Ergebnisse dieser Prüfung werden in einem Lauf- oder Prüfprotokoll (**Laufzettel oder Aktenvermerk**) festgehalten. Jede übermittelte Nachricht wird mit einer eindeutigen Identifikationsnummer - analog einem Eingangsstempel - versehen. Die eigentlichen Nutzdaten des inneren Umschlags können vom Intermediär nicht eingesehen werden. Diese kann und darf nur der eigentliche Empfänger einsehen und verarbeiten. Laufzettel und verschlüsselter Nachrichtentext werden solange beim Intermediär zwischengespeichert, bis sie durch den berechtigten Empfänger beim Intermediär abgeholt, bzw. angefordert werden. Wie lange ein Intermediär einen Laufzettel aufbewahren muss und der Status der Nachricht abfragbar ist, sind nicht definiert. Das Öffnen des inneren Umschlags erfolgt im Backendprozess, da nur dieser den zum Entschlüsseln der Nachricht notwendigen privaten Key besitzt.

Im Laufe des Projektes wurde es schnell ruhig um diese erste VPS, denn OSCAR war eben nur eine Anwendung, die gleichberechtigt neben anderen eGovernment- Anwendungen stand. Nach Abschluss des [Media@Komm-Projektes](#) lag dann als wichtigstes Ergebnis das neu geschaffene Nachrichten- und Transportprotokoll OSCI für eGovernment- Anwendungen vor. In dieser Form beschreibt OSCI eine Familie von Protokollen zur Standardisierung von Daten und deren Transport.

Mit Projektende wurde die Middleware der bremen online services GmbH & Co.KG (bos) **Governikus** genannt. Der Grund: Man hatte festgestellt, dass die Aufgabenverteilung (technisch: Rolle) von Sender, Intermediär und Empfänger einer Nachricht, so wie sie in HBCI vorgesehen waren, nicht identisch auf die eGovernment- Anforderungen zu übertragen waren. Man war gezwungen das Architekturmodell zu erweitern und OSCI diesen Gegebenheiten anzupassen. Das Nachrichtenprotokoll OSCI wurde in zwei Teile aufgeteilt. Im Teil A werden die Daten in einer geschäftsprozessbezogenen **XML- Struktur** be-

schrieben, in Teil B werden die Mechanismen für einen **sicheren Transport** dieser Daten definiert.

HEUTE

Die VPS des Bundes

Die Diskussion um die VPS wurde wieder lebhafter als das BMWi (Bundesministerium für Wirtschaft und Technologie) das Nachrichten- und Transportprotokoll OSCI als verbindlich für die *Virtuelle Poststelle des Bundes* - eine zentrale Komponente im Projekt **Bund Online 2005** - erklärte und IBM im Dezember 2002 in der *Anforderungsanalyse zum Konzept für die Virtuelle Poststelle als Basiskomponente Datensicherheit von Bund Online 2005* die notwendigen neuen Dienste und Schnittstellen beschrieb. Die Virtuelle Poststelle wurde jetzt als zentrales **Security-Gateway** gesehen. Über dieses „Sicherheitstor“ sollte die Kommunikation laufen. Die Kernkomponente (Governikus) soll über standardisierte Schnittstellen diejenigen **kryptographischen Sicherheitsdienste** bereitstellen, die für die gesicherte Kommunikation zwischen Behörden, externen Kommunikationspartnern, Bürgern, Wirtschaft und Handel notwendig sind.

Leitgedanke des Konzeptes ist: Es ist für das Ver- und Entschlüsseln ein- und ausgehender Nachrichten, für die Signaturprüfung, oder für die Prüfung auf schädliche Inhalte nur eine aufwändige technische Ausstattung an zentraler Stelle sinnvoll. Für den Betrieb und die Wartung ist ein umfangreiches technisches Know-how erforderlich. Die Middleware Governikus soll deshalb als Kernfunktionen dieser **VPS des Bundes** die nachfolgenden Sicherheitsdienste gewährleisten:

- Vertraulichkeit - der übertragenen und gespeicherten Informationen,
- Integrität - der übertragenen und gespeicherten Informationen,
- Verbindlichkeit - Authentizität und Nachweisbarkeit
- Authentifizierung - Unterstützung für Web-basierte und andere Anwendungen mit verschiedenen Authentifizierungsverfahren
- Monitoring und Auditing

Im Herbst 2004 ergänzte der Bund dann die Definition nochmals. Eine Virtuelle Poststelle im Sinne einer Basiskomponente von Bund Online 2005 soll:

- die Kommunikationssicherheit sicherstellen und - je nach Anspruch und organisatorischer Ausgestaltung - auch weitere Querschnittsfunktionalitäten bieten,
- sich nahtlos in den Webauftritt integrieren lassen,
- über standardisierte Binnen-Schnittstellen die Anbindung an Fachverfahren und externe Sicherheits-Komponenten möglich machen,
- flexibel an neue Organisationsformen, die Erfordernisse von Kooperationen mit Handel, Wirtschaft, Bürgern und anderen Behörden anpassbar sein,
- technisch als zentrales Security-Gateway dienen, und die Funktionen Authentifizierung, Signaturprüfung und Signaturerstellung sowie Ver- und Entschlüsselung bereitstellen,
- als Kommunikationskanäle sowohl E-Mail als auch Web- Anwendungen und darüber hinaus auch Web-Mail-Anwendungen ermöglichen,
- Schnittstellen zu Dokumentenmanagement-, Workflow- und Archiv- Systemen haben.

Während der Übermittlung sollen Mehrwertdienste schnell und vor allem transparent erbracht werden ohne dabei die Vertraulichkeit zu verletzen. Die VPS soll in der Rolle des Senders und Empfängers auftreten können.

Dieser große, zentrale Ansatz wird kontrovers diskutiert. Denn in der Folge bedeutete dieses Konzept, dass die komplexe Lösung sehr teuer ist, flexibel und offen ausgelegt werden muss und die notwendigen Schnittstellen zu den weiteren Kommunikationsservern und Diensten erst nach und nach entwickelt werden können. Gleichzeitig rückt das Konzept einen weiteren Problemkreis in den Mittelpunkt, für den es bis heute keine überzeugenden Lösungen gibt. Gesicherte e-mail-Kommunikation leidet an mangelhafter Interoperabilität. Sobald sensibler externer e-mail-Verkehr geschützt werden muss, wird die Sicherung und das Recover von e-mail-Daten zum Problem. Es wird schwierig eine Abbildung interner Ver-

treter-Regelung zu treffen, und die Viren-Problematik wirft neue Aspekte auf.

Arbeitsplatzbezogene Lösungen sind individuelle Konzepte. Sie benötigen so viele Schlüssel wie Mitarbeiter im Unternehmen sind. Scheidet ein Mitarbeiter aus, muss gewährleistet sein, dass berechnigte Personen die an den Mitarbeiter gerichteten oder von ihm bereits erhaltenen e-mails lesen können. Die Schlüssel der Mitarbeiter müssen entweder an zentraler Stelle hinterlegt werden oder jede e-mail muss zusätzlich mit einem Hauptschlüssel - also doppelt - verschlüsselt werden. Die gleiche Problematik gilt für die Vertretung bei Abwesenheit. Bei der Prüfung verschlüsselter e-mails auf Virenbefall sind aufwendige Umverschlüsselungen erforderlich, da Anti-Viren-Programme nur Klartext analysieren können. Durch den zentralen Ansatz sollen diese Probleme gelöst werden. Die Virtuelle Poststelle des Bundes ist überwiegend Middleware und eine Serverlandschaft. Für die Praxis in den Kommunen stehen hingegen Alternativen bereit.

Die VPS des Landes NRW

Ein Beispiel für diese Art von Virtueller Poststelle ist der Ansatz, der in NRW seit 2003 verfolgt wird. Die VPS in NRW kombiniert unterschiedliche Protokolle der Nachrichtenübermittlung. Sie sichert den unsicheren Bereich (Internet) durch OSCI ab, setzt diesen nach Erhalt und Signaturprüfung zur Weiterleitung im sicheren landesweiten Netz auf SMTP (**S**imple **M**ail **T**ransfer **P**rotokoll) um. In NRW steht der Empfang signierter Nachrichten im Vordergrund, die Rückantwort ist ausgeklammert. Ein solcher Lösungsansatz benötigt einen Verzeichnisdienst, der die Adressaten enthält, an die die Nachricht intern weiterzuleiten ist. Diese Funktionalität wurde geschaffen. Aus technischer Sicht benutzt NRW also einen OSCI nach SMTP- Konverter in Verbindung mit einem eigenen Verzeichnisdienst. Ähnliche, leicht modifizierte Ansätze sind in der Region Hannover, Bremen und Bremerhaven anzutreffen.

GOVELLO DER VIRTUELLE BRIEFKASTEN

Govello, der virtuelle Briefkasten der **bremen online services GmbH** (bos) ist eine einfaches und komfortables Kommunikationstool auf der Basis von Governikus. Die Clientanwendung hat die Funktionalität eines handelsüblichen e-mail-Programms. *Govello* kann OSCI-Nachrichten empfangen und versenden und Verzeichnisdienste nutzen. Die Nachrichten sind **Ende-zu-Ende** verschlüsselt. Es ist geplant, die Verzeichnisdienste der PKI-1-Verwaltung sowie weitere Verzeichnisdienste einzubinden. Wesentlich mitentscheidend dafür sind die konkreten Anforderungen der **Bund Online 2005** Dienstleistungen und die Ergebnisse des **Media@Komm-Transfers**.

Durch die Flexibilität der Anwendung ist es möglich, individuelle Modifikationen einer Virtuellen Poststelle zu erstellen, beispielsweise das „Elektronische Gerichts- und Verwaltungs-Postfach“ (EGVP). Durch weitere Anpassungen von *Govello* ist es möglich, Virtuelle Poststellen für Einwohner- und Standesamtswesen zu entwickeln.

CuriaPOST

Die Anwendung **CuriaPOST** ist ein alternative VPS. Sie wird von der Firma **Curiavant Internet GmbH** vertrieben. **Curia-POST** wurde in der Media@Komm-Region Nürnberg entwickelt und benutzt ebenfalls das OSCI-Transportprotokoll. Im Gegensatz zu dem Ansatz der bremen online services GmbH & Ko.KG (bos), bei dem auf der Clientseite immer ein Java-Programm zum Einsatz kommt, setzt Curiavant auf webbasierte Lösungen. Voraussetzung für diesen Ansatz ist jedoch, dass als Middleware die eGovernment-Infrastruktur **Curia-World** eingesetzt wird. Die Middleware CuriaWorld stellt alle wichtigen Querschnittsfunktionen im Backend, als vor den eigentlichen Fachverfahren zur Verfügung, während diese Funktionalität bei Governikus durch den Intermediär erbracht wird.

AN DER BASIS

Die Diskussion erreichte in dieser Phase auch die Kommunen. Denn das BMWI initiierte das Projekt [Media@KommTransfer](#).

Unter dem Leitgedanken Standardisierung und Harmonisierung sollten ausgewählte Transferkommunen ihre spezifischen Anforderungen an eine VPS definieren, abstimmen und als Handlungsempfehlungen verbreiten. Virtuelle Poststelle, Formularserver, Dokumentenmanagementsysteme (DMS) und Contentmanagementsysteme (CMS) sind zu aktuellen Begriffen in der Diskussion um eine kommunale VPS geworden. Das Zusammenspiel mit anderen Anforderungen wie OSCI-Transport, Datensicherheit und Datenschutz ergibt jetzt einen unübersichtlichen Mix.

Es gilt Sicherheitsfunktionen zu definieren und Anwendungsszenarien durchzuspielen, die organisatorisch mit Funktionen der bisherigen analogen Posteingangsstellen vergleichbar sind. Diese sind in weiteren Schritten den technischen Gegebenheiten anzupassen.

Es sind die Fragen zu beantworten:

- Welche ausbaufähigen und zukunftssicheren Lösungen braucht eine Kommune wirklich?
- Wie gewährleistet eine Kommune IT-Sicherheit und Datenschutz?
- Bis zu welcher Stelle setzt eine Kommune auf OSCI?
- Wie sieht ein tragfähiger Kompromiss zwischen Anforderung und finanziell Machbarem aus?
- Wann ist eine Ende-zu-Ende-Kommunikation und wann eine behörden- oder funktionsbezogene Kommunikation erforderlich?
- Welche Systeme sind für die spezifischen Anforderungen in der Verwaltung geeignet?
- Welcher grundsätzlichen Integrationsrichtung sollen die Kommunen folgen?

Diese grundsätzlichen Fragen sowie vertiefende technische Erklärungen zu der Basistechnologie werden in einer späteren Ausarbeitung untersucht.

** Der Verfasser ist beim Informations- und Kommunikationsinstitut der Stadt Saarbrücken (IKS) im Bereich e-Government und EU-Projekte tätig.*